Azure AD Application and DevOps Integration



John Savill
PRINCIPAL CLOUD SOLUTION ARCHITECT

@NTFAQGuy www.savilltech.com



Module Overview



Using service principals

Leveraging managed identities

Assigning roles to service principals

DevOps service connection usage



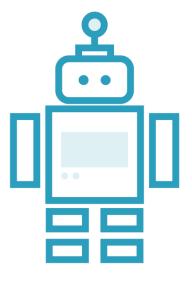
Applications need access to other resources so need to authenticate to be authorized.



Application Authentication



Service Principal



Managed Identity



Service Principals



Service principal is an account in Azure AD that represents an application instance in a tenant

Service principals can for authentication

- Secret
- Certificate

Requires management, storage and rotation of the secret

az ad sp create-for-rbac --name "<name>" --role contributor
--scopes /subscriptions/<sub id>/resourceGroups/<resource
group> --sdk-auth

Add --cert for certificate-based authentication

Creating Service Principal

Can create using PowerShell as well using New-AzADServicePrincipal

Using Managed Identities

Removes the need for manually managed application service principals and the considerations related to having passwords in code or authenticating to key vaults

Provides Azure services with an automatically managed identity

Available for a number of services including Windows/Linux VMs, App Services and Functions

Application within the resource utilizes special endpoint to leverage the managed identity

System and user assigned available

DevOps Service Connections

DevOps solutions will often need to interact and deploy Azure resources

Service principals are created to represent the DevOps instance

Appropriate Azure roles should be granted to the principal to enable the required deployments

Both Azure DevOps and GitHub Actions support the SDK authentication file format and secure storage as secrets

Summary



Using service principals

Leveraging managed identities

Assigning roles to service principals

DevOps service connection usage



Thank you and good luck!

